REMARKS

The specification has been amended to overcome a grammatical omission through the addition of the word "to" between the words "sufficient" and "establish" on p. 6, line 22 of the specification; and to change the word "in" to be the word "is" between the words "SPI-in" and "a" at p. 7, line 4 of the specification to give proper meaning to the sentence. The amendments do not add new matter, and do not change the meaning of the specification.

In the Office Action, the Examiner indicated that formal drawings would be required. New formal drawings are included in this Response and Amendment.

In the Office Action, claims 1 – 7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Awadallah et al. (6,449,251 B1) in view of Boden et al. (6,615,357 B1) in further view of Stevens (TCP/IP Illustrated). In particular, the Examiner found that the limitation in claim 1, that requires:

> a plurality of internal tables associating combinations of local IP addresses of local devices on said LAN, external IP addresses of external devices on said external network . . . source port addresses, destination port addresses, reserved port addresses, and maintaining a list of reserved port addresses . . .

is met by Awadallah et al. on column 4, lines 30 – 33 and column 2, lines 26 – 29. Other claim limitations said to be found in Boden et al. and Stevens were also noted. It was the Examiner's opinion that the combination of references disclosed each element of claims 1 – 7, and that it would have been obvious to a person of ordinary skill in the art to combine the references to arrive at applicant's invention.

Claims 2 – 7 were rejected over various combinations of Boden et al., Awadallah et al., and Stevens.

Claims 8, 10 and 18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Awadallah et al. in view of Stevens. In claim 8, the limitation:

> maintaining a plurality of tables associating local IP addresses of local devices on said LAN, external IP addresses of external devices on said external network, port addresses of said local devices, port addresses of said external devices, SPI-In values, SPI-Out values, and reserved port addresses, and a list of reserved port addresses . . .

was found to be met by Awadallah et al. on column 2, lines 26 – 29 and 62 – 64, and column 4, lines 30 – 33. The limitation "receiving a datagram from said LAN" is met by Awadallah et al. at column 3, lines 64 – 67 and column 4, lines 1 – 4. The limitation:

> determining whether the destination port address for said datagram is included in said table of reserved port addresses and, if said destination port address is not included in said table of reserved port addresses, performing normal address translation upon said datagram and passing said datagram to said external network for routing and delivery to said external device . . .

was found to be met by Awadallah et al. at column 3, lines 61 – 67 and column 4, lines 1 – 4. The limitation:

> and if said port address is included in said table of reserved port addresses, determining whether said destination port address is bound to an IP address, and if said destination port is bound to an IP address, performing normal address translation upon said datagram and passing said datagram to said external network for routing and delivery to said external device, and if said destination port address is not bound to an IP address, modifying said source IP address to be said external IP address for said external device, binding said destination port address to the local IP address of said local device and creating an association between said destination port address and said external IP address of said external device, and passing said datagram to said external network for routing and delivery to said external device . . .

is inherently met by Stevens on Section 3.3, page 37 – 38, 1st paragraph. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Stevens within the system of Awadallah et al. because the IP routing procedure is a

basic routing procedure performed by a router/gateway to a host that is either within a LAN or that needs to be reached outside the LAN.

Claim 10 was found to have limitations that are the "reverse" of those in claim 8, and was rejected on the same grounds as claim 8.

The limitation of claim 18, that:

> a machine readable storage, having stored thereon a computer program having a plurality of code sections executable by a machine and for connecting a LAN to an external network via a network address translating gateway, wherein said gateway having a local IP address that can be seen by devices on said LAN and having an external IP address that can be seen by devices on said external network, and further including a plurality of internal tables associating combinations of local IP addresses of local devices on said LAN, external IP addresses of external devices on said external network, source port addresses, destination port addresses, reserved port addresses, and a list of reserved port addresses, for assisting the machine . . .

was found to be met by Awadallah et al. on column 2, lines 26 – 29, column 3, lines 60 – 67, and column 4, lines 1 – 8 and 30 – 33. The limitation in claim 18 of:

> determining whether the destination port address for said datagram is included in said list of reserved port addresses and determining whether said destination port address is bound to said local IP address of said local device performing normal address translation upon said datagram and passing said datagram to said external network for routing and delivery to said external device if said destination port address is not included in said list of reserved port addresses

is said to be met by Awadallah et al. on column 3, lines 60 – 67 and column 4, lines 1 – 4. The limitation:

> performing normal address translation upon said datagram and passing said datagram to said external network for routing and delivery to said external device, if said destination port address is included in said list of reserved port addresses and if said destination port address is bound to said local IP address; and modifying said source IP address of said datagram to be said external IP address of said gateway, binding said destination port address to said local IP address of said local device and creating an association between said destination port address and the external IP address of said external device, and passing said datagram to

said external network for routing and delivery to said external device if said destination port address is not bound to said local IP address of said local device

is said to be met by Section 3.3 of Stevens, at p. 37 – 38, 1st paragraph. According to the Examiner, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of Stevens within the system of Awadallah et al. because the IP routing procedure is a basic routing procedure performed by a router/gateway to a host that is either within a LAN or that needs to be reached outside of the LAN.

Claims 9 and 11 – 17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over various combinations of Awadallah et al. in view of Stevens in further view of Boden et al.

On March 24, 2004, applicant's counsel met with the Examiner, the Examiner's Supervisor, and others. During that interview, applicant's counsel pointed out differences between applicant's invention and the prior art of record. Unlike Boden et al., applicant's invention applies to the use of IPSec protocol in transport mode in which IPSec processing is performed at a host device rather than at a gateway to a local area network. Applicant's invention permits the use of an ESP (encryption) header which does encrypt the payload of an IPSec packet, but does not encrypt source or destination IP addresses or SPI values in datagram headers. Because the gateway of applicant's invention can read and process IP addresses, network address translation can be carried out upon IPSec packets using ESP headers while passing through the encrypted payload without modification.

Applicant's invention also permits the establishment of security associations (SA's) through in-the-clear transmissions using ISAKMP protocol. The IANA (Internet Assigned Numbers Authority) has assigned (reserved) specific port addresses for specific application processes. For ISAKMP transmissions, port 500 must appear as both the source and destination

port addresses or the datagram will not be recognized as an ISAKMP transmission. Other process-specific port addresses may be used for other applications, such as games and the like, as explained in the specification. Because ISAKMP protocol requires that datagrams have port 500 as both source and destination port addresses, applicant's invention does not translate those port addresses during ISAKMP transmissions, thereby allowing the sending and receiving devices to verify that an ISAKMP protocol is being used. In order to "pass-through" the ISAKMP datagrams without translating the port addresses, applicant's invention determines when a host on the LAN has initiated an ISAKMP process, passes the datagram without translating the source port address, binds the process-specific port to the IP address of the local host, and retains the binding until a return datagram having source and destination port addresses of port 500 is received, or a predetermined length of time has expired. While the binding is being retained, the gateway will not pass an ISAKMP datagram from any other computer on the LAN, and no ISAKMP datagram from the external network will be passed through the gateway unless it originated from the same external IP address that the earlier ISAKMP datagram was sent to. Thus, applicant's invention is distinguished from Boden et al. by "passing-through" ISAKMP datagrams without translating port addresses while performing normal address translation for all other datagrams. By contrast, Boden et al. does all IPSec processing at the gateway, and encapsulates datagrams from the LAN as the payload of a datagram having an IPSec header.

During the interview, the Examiner pointed out that Awadallah et al. also uses tables of port addresses that are "reserved," and that applicant's "reserved port addresses" in claims 1, 4, 8, 10, and 18 are thereby made obvious by Awadallah et al. Awadallah et al., however, does not disclose or teach the use of a list of process-specific ports, such as port 500 for the ISAKMP protocol. Moreover, Awadallah et al. uses port addresses and "reserved" ports for determining

packet prioritization rather than for process-specific filtering. *See, e.g.*, Awadallah et al. at col. 3, lines 48 – 56: "This packet mapper in network edge routers monitors the port number negotiation and selection for those applications and protocols that dynamically select data exchange port numbers, maintains a proxy table that maps dynamic port numbers to reserved port numbers for high priority traffics, and finally intercepts those data packets with dynamic port numbers and performs port swapping before routing these packets to the next hop router, and vice versa." Applicant's invention does not perform these functions, nor do Awadallah et al's "packet mapper" perform the function of detecting process-specific port addresses to "pass through" the gateway without being translated.

Claims 1, 4, 8, 10, and 18 have now been amended to refer to "process-specific" port addresses, which are disclosed in the applicant's specification. *See, e.g.*, p. 8, lines 3 – 5, and p. 25, line 22 – p. 26, line 5. During the interview, applicant and the Examiner agreed that the claims would be amended to more particularly define the differences between the prior art and applicant's invention. As amended, the independent claims do not read on the prior art, and would not have been obvious to a person of skill in the art at the time the invention was made.

The preamble to claim 1 has been amended to substitute the word "referenced" for the word "seen" to clarify that the network address translating gateway is electronically situated between the local area network (LAN) and the external network, and has local and external IP addresses that can be referenced by devices on either respective network.

The fifth and sixth paragraphs of claim 1 have been amended to delete references to "said local IP address of said local device," and to substitute "a local IP address." The words "for routing and delivery to said external device" have also been deleted. These changes are supported at p. 17, lines 8 to 16 of the specification, where Port 500 is described as being bound

to "some other local IP address" (rather than to the IP address of "said local device" ); and the datagram is then processed and dispatched, but will be rejected by the external device, hence may be considered not to undergo "routing and delivery to said external device."

Claims 2 and 3 were previously amended in the first Preliminary Amendment, and remain unchanged in this Amendment and Response.

Claim 4 has been modified to conform to the specification at p. 18, line 18 – p. 19, line 5. This is done by substituting the words "the local IP address of said local device" with the words "a local IP address"; and by adding the words "determining whether said destination port address is associated with the external IP address of said external device, and if said destination port address is associated with the external IP address of said external device . . ."

As explained in the specification, a datagram coming to the gateway from the external network will not have in its destination IP address field the local IP address of the local machine to whom the datagram is intended, and the gateway cannot initially know which local machine should receive the datagram. The gateway requires two steps to make that determination: First, the gateway must check to see whether the destination port (Port 500) is bound to <u>any</u> local IP address. If the port address is not bound, then the datagram will be discarded. If the port is bound, the gateway must next determine whether that binding is associated with the external (source) IP address contained in the datagram. If both of these conditions are met, then the gateway will send the datagram to the local IP address that is bound to the port. The modification to claim 4 clarifies that the gateway initially senses only that the port is bound to <u>some</u> local IP address; without knowing specifically whether it is the local address of the intended recipient of the datagram. If the port is bound, then claim 4 requires the gateway to see

whether the binding is associated with the proper source IP address. If it is, then the gateway will pass the datagram to the LAN for delivery to the intended recipient.

Claims 5 – 7 were previously amended in the first Preliminary Amendment, and remain unchanged in the Second Preliminary Amendment.

Claim 8 has been amended in the same manner as claim 1 through deletion of the words, "for routing and delivery to said external device"; This modification is necessary to clarify that the external device will not accept a packet having a source port address of 500 and an arbitrary (translated) destination port address.

Claim 8 has also been modified to correct an error that appeared in the first Preliminary Amendment by changing the datagram's source address to be the IP address of the gateway, rather than the IP address of the external device to whom the datagram is being sent.

The specification explains that, for an outgoing ISAKMP datagram, if port 500 is not bound, the gateway will bind port 500 to the local IP address of the sending machine, and will create an association between that binding and the external IP address of the intended recipient. It will also modify the source address for the outgoing datagram to be the external IP address of the gateway, and claim 8 has been modified to show this.

Claim 9 was previously amended in the first Preliminary Amendment, and remains unchanged in the Second Preliminary Amendment.

Claim 10 is a method claim whose subject matter is analogous to the subject matter of apparatus claim 4. Changes to claim 10 are made for the same reasons as those made to claim 4.

Claim 11 has been amended to substitute the word "local" for the word "internal." This amendment simply corrects a typographical error that was introduced in the first Preliminary Amendment.

Claim 12 has been amended to correct the claim from which it depends.

Claim 13 is redundant, and is therefore being canceled.

Claim 14 was newly added in the first Preliminary Amendment and remains unchanged.

Claim 15 has been amended to correct an anomaly that was introduced when the Preliminary Amendment was converted from a WordPerfect document to a Microsoft Word document, prior to having been submitted in the first Preliminary Amendment. The Preliminary Amendment, including claims 15 and 16 as amended herein, had originally been drafted in a WordPerfect document. During conversion of the document from WordPerfect to Microsoft Word, some lines that included the end portion of claim 15 and the beginning portion of claim 16 were dropped. The error was not discovered until after the Preliminary Amendment had been filed. As amended, claim 15 depends from claim 11, and is fully supported in the specification at page 14 and in Figure 1.

Claim 16 is missing from the Preliminary Amendment (although a claim 16 was included in the Extra Sheets Containing Marked-up Claims, it was not included in the body of the amendment, and should not constitute part of the Preliminary Amendment.) This anomaly is due to the conversion of documents prior to the submission of the Preliminary Amendment. Because claim 16 is missing from the application, applicant notes that, with the addition of new claims 19 – 21, there should be no additional charges for claims in excess of 20 because claim 16 was omitted from the Preliminary Amendment.

In the event the Examiner deems that additional fees for excess claims are due, the Examiner is requested to charge any additional fees against applicant's counsel's Deposit Account, Acct. No. 500,951.

Claim 17 was newly added in the first Preliminary Amendment and remains unchanged in this Response and Amendment.

Claim 18 was newly added in the first Preliminary Amendment, and has been amended in this Response and Amendment to improve the grammatical syntax and clarify and better define the subject matter of the claim. Amendments to claim 18 also include modifications similar to those previously explained with reference to currently amended claim 4.

No new matter has been added to the application.

Respectfully submitted,

Michael C. Cesarano
Reg. No. 31,817
Cust. No. 26058
mcesarano@akerman.com

AKERMAN, SENTERFITT
Suntrust International Center, 28th Floor
1 S.E. 3rd Avenue
Miami, Florida 33131-1714
305-374-5600 Telephone
305-374-5095 Telefax

Dated: April 15, 2004